A White Paper from the Experts in Business-Critical Continuity™

Power and Cooling Design Guidelines for Network Access Rooms

EMERSON™
Network Power

Introduction

Network access and telecom rooms are housing more powerful and critical equipment as businesses rely on these spaces to support an increasing number of business-critical applications. The technologies supporting the deployment of IP telephony, wireless networking, converged applications, and other equipment outside traditional IT data storage and management are finding their way into nontraditional spaces that weren't designed as data centers. These rooms also support important operational functions including time and attendance equipment, building maintenance alarms and security equipment. In the event of a failure within a network access room, organizations may be susceptible to the disruption of revenue-generating activities or the inoperability of security and phone systems, among other serious consequences.

Because network access equipment has traditionally been housed in converted closets or other spaces not well suited for electronics, its reliability and that of newer devices has been placed in jeopardy. These spaces often constrain growth or enhanced use of the closet because of the lack of physical space and power/cooling infrastructure required to support the powerful and critical equipment on which the business is now dependent (Figure 1).

More powerful equipment generates more heat. When the equipment is trapped in a small, poorly ventilated space, heat can quickly raise the temperature to unsafe levels that reduce performance and shorten equipment life. Additionally, the hardware running these applications requires higher availability power protection through an uninterruptible power supply (UPS) system.

Threat to Business Continuity

For example, Voice over Internet Protocol (VoIP) can change the economics associated with network access downtime by adding significant costs to a business should there be a disruption. When evaluating the criticality of network and telecom closets, IT managers should review applications supported by the network and evaluate the impact to the business if those applications become unexpectedly unavailable. Addressing costs associated with employee productivity and revenue-generating activities should not be overlooked. As downtime costs rise, so too should the investment in technologies that can increase availability.

Configuring the appropriate solution involves both overcoming the physical challenges imposed by the space and understanding the cost of downtime for the environment. The good news is that there are solutions available today that allow powerful and sensitive network equipment to operate safely and reliably in almost any environment.

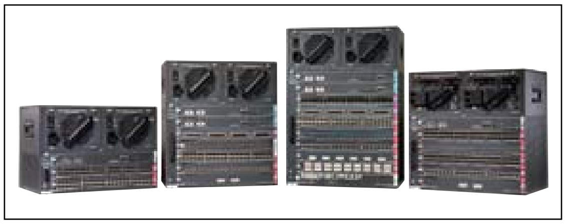

Figure 1. New switches, routers and other equipment being deployed as part of an IT system upgrade may require enhanced power and cooling support.

Evaluating the Physical Environment

The network access room environment poses a number of challenges for power, cooling and monitoring systems. Evaluation of the network closet's size and existing power and cooling attributes will help ensure that it is designed with solutions that can easily support growth and flexibility as business needs change.

More powerful equipment generates more heat. When the equipment is trapped in a small, poorly ventilated space, heat can quickly raise the temperature to unsafe levels that reduce performance and shorten equipment life.

Size
The small size of network access rooms can limit power and cooling equipment configurations. Most network access room installations require UPS systems that will take at least 2U of rack space, not including extended runtime batteries.

Existing Cooling
Cooling and ventilation will determine how effectively heat can be removed from the rack and from the access room. Equipment type and access room size will largely determine cooling requirements. Simple ventilation may suffice, or a dedicated cooling system may be warranted. Initial considerations should include ventilation of the access room, ducting of walls and ceilings, and year-round availability of building air conditioning.

Existing Power
When evaluating a room to handle network equipment, check out elements of the room's existing power supply to see if it can adequately support the technologies that it may house.

The size and number of circuits required are determined by power usage and redundancy requirements. Support for Power over Ethernet (PoE) can quadruple power requirements. Certain redundancy strategies, such as "dual bus" may require more than one circuit for UPS systems. If additional circuits must be added, it is wise to provide some room for future growth as new PoE standards will allow the format to support higher-powered devices such as laptops.

Also, the type of wall receptacles in the access room will impact compatibility with UPS systems. For example, UPS systems with capacities of more than 2,000 VA have different plug types that may not fit the commonly used 15 amp or 20 amp receptacles in network access rooms.

These factors, along with building layout and network equipment criticality, will drive the decision on whether to use centralized or decentralized UPS systems. Some organizations may be able to utilize a single UPS located in a computer room to protect network access rooms throughout the same building. The advantages of a centralized UPS with larger, more robust technology include lower cost of ownership and higher system availability because of fewer potential points of failure and easier management (Figure 2). This approach also simplifies service and maintenance requirements.

The advantages of a centralized UPS with larger, more robust technology include lower cost of ownership and higher system availability because of fewer potential points of failure and easier management. This approach also simplifies service and maintenance requirements.

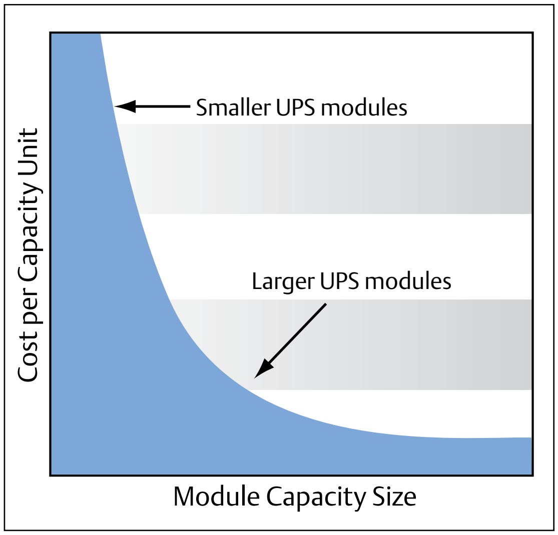

Figure 2. Larger UPS modules leverage economies of scale to drive down the cost per kW.

Others may adopt a decentralized strategy in which UPS systems are located in each rack or access room. Advantages of this strategy include simpler installation and lower initial cost. Highly reliable, rack-mounted, line-interactive and double-conversion UPS systems are available from 700 VA to 10 kVA, making it practical to deploy power protection in almost any environment housing rack-mount servers, switches and routers. Also, new 208V UPS systems increase the ability of IT and network managers to adapt to the requirements of modern applications and IT equipment, including servers, routers and switches that can handle either 120V or 208V power with no modifications necessary. If decentralized power protection is used, be sure to account for UPS losses when determining room power requirements.

Determining Network Hardware Requirements

Network hardware required for converged applications will require a high-availability infrastructure that may have more in common with systems used in the data center rather than those traditionally used in network access rooms.

Achieving High Availability Protection

High availability protection for network access rooms can be realized through deployment of reliable, flexible and cost-effective solutions that provide necessary levels of power quality, power reliability, cooling and ventilation, remote monitoring and management, physical security, and preventive maintenance and rapid response service.

In many instances, most of this critical network equipment will be stored together in a rack. It's imperative to use a rack equipped with ease-of-use design flexibility that allows for the quick installation of new technologies. Physical security will be enhanced with a locking door, which should be perforated to improve airflow to reduce heat, helping to ensure higher availability.

Power Quality

The criticality of the network equipment will determine the type of UPS required. Does the network equipment only need power backup during outages or does it require continual power protection and conditioning? Again, VoIP may elevate network criticality. Whereas power availability for phone systems was traditionally provided by phone companies, today it is the responsibility of each organization. Converged applications should be supported with higher power availability – up to 99.9999 percent – to withstand between 31 seconds and 5.2 minutes of total annual downtime.

Most general network access applications use a line-interactive UPS, such as the Liebert PSI. This type of UPS provides extended battery capacities, some power conditioning, and delivers solid backup power protection for a wide variety of applications if full power conditioning or a fault-tolerant design is not required.

For business-critical, always-on applications, a true online, double conversion UPS, such as the Liebert GXT, is a preferred choice. A double conversion UPS delivers a lower total cost of ownership, provides highly effective power conditioning, and relies less on the battery system to correct for power anomalies, extending battery life. It also protects against UPS component failures, including premature battery failure from overheating, power overload and failure of the internal inverter. True online UPS units have higher reliability than line-interactive systems because they include a fault-tolerant design with an internal bypass that maintains power during any of the above circumstances.

Midsize, three-phase UPS systems, such as the Liebert NX (Figure 3), can provide highly reliable centralized power protection for multiple network access rooms from a single location. These systems can introduce capabilities not available in smaller UPS systems, such as software scalability, which allows capacity growth without adding hardware, and uneven paralleling, which permits different size modules to operate in

High availability protection for network access rooms can be realized through deployment of reliable, flexible and cost-effective solutions that provide necessary levels of power quality, power reliability, cooling and ventilation, remote monitoring and management, physical security, and preventive maintenance and rapid response service.

Several important considerations including UPS sizing, runtime requirement, power distribution and power redundancy, must be evaluated to achieve desired levels of power reliability.

Figure 3. The Liebert NX is a midsize, three-phase UPS designed for scalability.

parallel. These features work together to enable a clear, easy-to-manage path for adding capacity or redundancy.

Power Reliability

Reliable power is the lifeblood of fully functioning network access rooms. Based on the increasing criticality of applications relying on the technologies powered in these rooms, any power abnormalities have the potential to thwart business continuity. Therefore, several important considerations including UPS sizing, runtime requirement, power distribution and power redundancy, must be evaluated to achieve desired levels of power reliability.

UPS Sizing

When sizing the UPS for a network access room, use full load calculations for protected equipment to help ensure adequate power and allow for growth. Some organizations use nominal loads or estimate their average loads, which could result in undersized UPS units leading to critical equipment downtime. With the changing nature of network technology and growth in power requirements, sizing the UPS units to accommodate a 50 to 100 percent growth factor is not excessive.

If PoE is being used, power usage calculations must account for the inline power to the network devices (Figure 4). Remember that PoE draws could grow from the current 15 watts per port to 40 watts per port as new PoE standards emerge. As a result, power densities in network access rooms are often three to five times greater than traditional network equipment, which will require larger or additional UPS systems.

Runtime Requirements

Runtime requirements will vary based on equipment criticality. Organizations wanting to support graceful shutdown of equipment may only need a few minutes of runtime. Conversely, organizations wanting to ensure continuity of critical applications may need two hours or more, which requires additional batteries. It's important to note that battery systems may require additional space if extended runtime (beyond five minutes) is required.

Power Distribution

Power distribution is important for ensuring power reliability. Rack-level power distribution units (PDUs) provide basic receptacle-level power distribution and high capacity designs for high-end switches.

Additionally, intelligent power strips can support remote power control as some products provide on-off operation of individual receptacles. This feature can be used to limit how much equipment is plugged

Cisco Catalyst Model	Data Power (Watts)	PoE Ports	PoE Power (Watts)	Total Power (Watts)
4503	405	48	830	1235
4507r	920	144	2491	3411
4510	1200	288	4962	6162

Figure 4. Using Power over Ethernet changes network access room power requirements.

into the UPS, reducing the risk of circuit overload and ensuring that only authorized equipment can be powered up.

Power Redundancy

Power redundancy has become more important with the growth of high-availability applications as organizations seek to reduce single points of potential failure. Most network equipment now comes with multiple power cords to support redundancy. A redundancy strategy should be driven primarily by availability requirements.

In a single UPS configuration (Figure 5), both cords are plugged into the same power distribution unit, which is then plugged into a single UPS connected to the wall outlet. While the UPS provides backup if the utility power fails, there is no UPS redundancy in case the UPS fails.

To protect against UPS failure, one cord of the rack equipment may be plugged into the wall receptacle, with the other cord plugged into the PDU connected to the UPS (Figure 6). This configuration allows incoming power to provide redundancy in the event of a UPS failure but exposes the network to potential utility loss.

Using a single UPS with a maintenance bypass and power distribution switch is a low cost way to protect against utility loss. With this configuration, each equipment cord goes to a separate PDU with each PDU plugged into

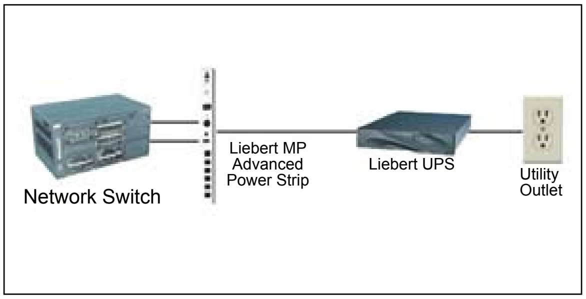

Figure 5. Single UPS configuration.

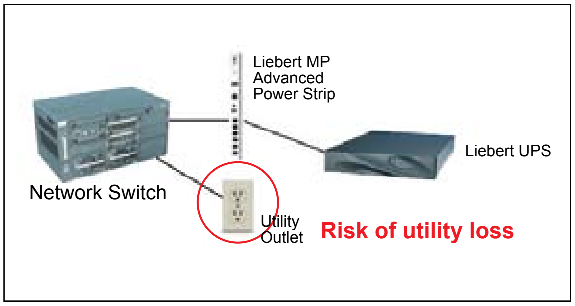

Figure 6. Single UPS with utility power.

the maintenance bypass switch (Figure 7). One cord from the maintenance bypass switch is plugged into the wall and the other cord is connected to the UPS.

This configuration allows power to be provided from the UPS to rack equipment in the event a utility power outage occurs. Power can also be provided from the wall if a UPS fails or while the UPS is being maintained. Although this solution is certainly better than a standalone UPS, it does not provide UPS backup redundancy.

For true high availability applications, UPS redundancy should be considered. Figure 8 shows a power redundancy configuration that can be deployed in network closets; the configuration includes a PDU positioned between the protected devices and the UPS. The highest availability is achieved with a dual bus system. With this configuration, equipment cords are plugged into separate

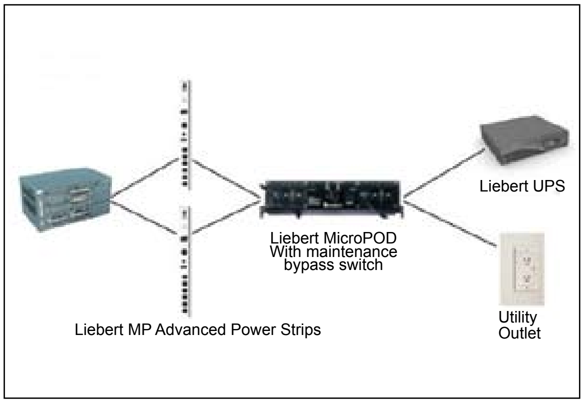

Figure 7. Single UPS and Maintenance Bypass Switch.

For true high availability applications, UPS redundancy should be considered. The highest availability is achieved with a dual bus system.

When planning the cooling system, determine whether the door, ceiling or walls can support ductwork for ventilation and whether the heat can be exhausted to the outside.

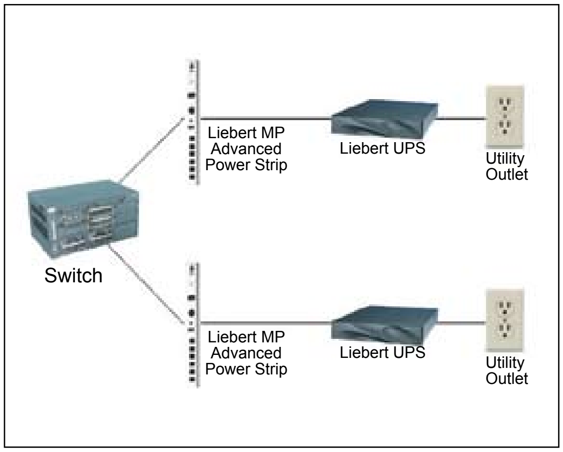

Figure 8. UPS redundancy with the dual-bus approach provides the highest availability.

PDUs and the PDUs are plugged into separate UPS units. In turn, the UPS units are plugged into separate circuits. A dual-bus configuration provides UPS backup redundancy during a power outage and up to nine "9s" of power availability, which translates into just 3/100 of a second of potential downtime each year.

Cooling and Ventilation

Today's power-hungry switches generate more heat than previous generations of equipment. As a result, rack temperatures often exceed safe operating levels and because the heat will not dissipate, it must be removed from the rack and the room. Heat that is not removed will be drawn back into the rack.

Cooling requirements depend primarily on the equipment type and room size. In cases where switch power requirements are low, simple ventilation may suffice. Higher density equipment will typically require a dedicated cooling system. In fact, the Uptime Institute has reported that equipment located in the top one-third of a data center rack fails twice as often as equipment in the bottom two-thirds of the same rack. The organization estimates that for every increase of 18 degrees F above 70 degrees F, long-term electronics reliability falls by 50 percent.

When determining cooling requirements, those responsible for the environment should evaluate the existing cooling system as noted previously, and determine whether the space has dedicated air conditioning or relies on the building air conditioning system or ventilation.

When planning the cooling system, determine whether the door, ceiling or walls can support ductwork for ventilation and whether the heat can be exhausted to the outside. If the closet is cooled by the building's air conditioning system, cooling is probably insufficient because building air conditioning systems cycle on and off and do not run throughout the year.

Figure 9 shows options for cooling and ventilation. For equipment loads of 100 watts to 1,000 watts, ventilating the closet space should be adequate. This should be accomplished without compromising the physical security of the space, which may require the installation of intakes and exhaust grills on the closet door.

Total Heat Load	Recommended Cooling Solution
< 100 Watts	Leaks and wall conduction
100 – 1000 Watts	Intakes and exhaust grilles in doors or walls
1000 – 5000 Watts	Dedicated cooling with remote heat rejection
> 5000 Watts	High heat density cooling with remote heat rejections

Figure 9. Cooling requirements are determined by equipment power consumption.

Rack fans provide another inexpensive method of removing heat from equipment with the closet ventilation removing it from the space.

Rooms with more than 1,000 Watts of equipment will need some form of dedicated cooling. Self-contained cabinets or rack enclosures, such as the Liebert MCR (Figure 10), are available that include support systems such as computer grade air conditioning, a UPS, monitoring capabilities and security features. If rack power is likely to exceed 5 kW, a high heat density cooling option such as the Liebert XDF (Figure 11) may be best, although the system will require proper ventilation of the closet space to remove condenser heat. This energy-efficient solution utilizes digital scroll compressors to automatically match cooling requirements to the heat load at any time, which ensures the cooling unit is not always running at full capacity.

Remote Management and Monitoring

While most organizations want to minimize the cost of physically inspecting and maintaining equipment in network access rooms, they want to be able to detect any adverse trends before they turn into emergencies. Remote monitoring and management software has the capability to identify adverse changes in the environment and equipment, including shifts in heat and humidity, water leaks, fluctuations in UPS input power, declines in battery capacity, and changes in runtime and output load percentage, as well as cooling equipment status.

Network management software can be used to determine the status of cooling equipment and automate the graceful shutdown of equipment in the event of a prolonged power outage. It can also reboot network equipment and control power usage at the rack PDU receptacle level to ensure adequate total capacity. For example, the Liebert Nform management software can initiate safe shutdown of critical equipment if absolute maximum temperatures are reached within the network closet.

For organizations using network management software, communication cards are available that allow power (including batteries) and cooling equipment data to be compiled and analyzed (Figure 12). This tool also provides the ability to remotely cycle the UPS on and off. In addition, small monitoring units can be integrated into the system to provide

Figure 10. Self-contained cabinets provide an easy-to-deploy integrated power and cooling solution for low heat density network access equipment.

Network management software can be used to determine the status of cooling equipment and automate the graceful shutdown of equipment in the event of a prolonged power outage. It can also reboot network equipment and control power usage at the rack PDU receptacle level to ensure adequate total capacity.

Figure 11. The Liebert XDF is a secured enclosure with integrated high heat density cooling, providing the benefits of big room support. Optimized horizontal air circulation cools the protected equipment both in standard and backup ventilation modes.

real-time monitoring of temperature and humidity changes, contact closures and water leaks.

Physical Security

Because network access rooms escape the scrutiny common to computer rooms, physical security is often a major issue. This is why it is important to make sure ventilation is not dependent on keeping doors open, which could allow unauthorized access. Simply, it is important to secure access room doors and secure equipment inside lockable cabinets. Also, various mechanical locking systems are available to enhance the physical security within network access room cabinets. Some cabinets include easy to use 3-cylinder combination locks to control access, with options available that allow access to be monitored via the customer's network.

Preventive Maintenance and Rapid Response Service

Preventive maintenance and service are critical to ensure the availability of network equipment. A number of options are offered to help meet maintenance and availability objectives, including maintenance bypass switches, environmental monitoring products, warranties, and remote monitoring and on-site services.

When selecting network access room equipment, it is essential to understand the parameters of the product warranty. If a component fails, will the company replace the UPS overnight via 24x7 customer support? And, will the warranty cover shipping both ways?

Some companies offer inexpensive one- and three-year extended warranties at the time of purchase that can cost effectively lengthen the life of the UPS. Depending upon the warranty, on-site and preventive maintenance services may be included, with remote monitoring and other services also available.

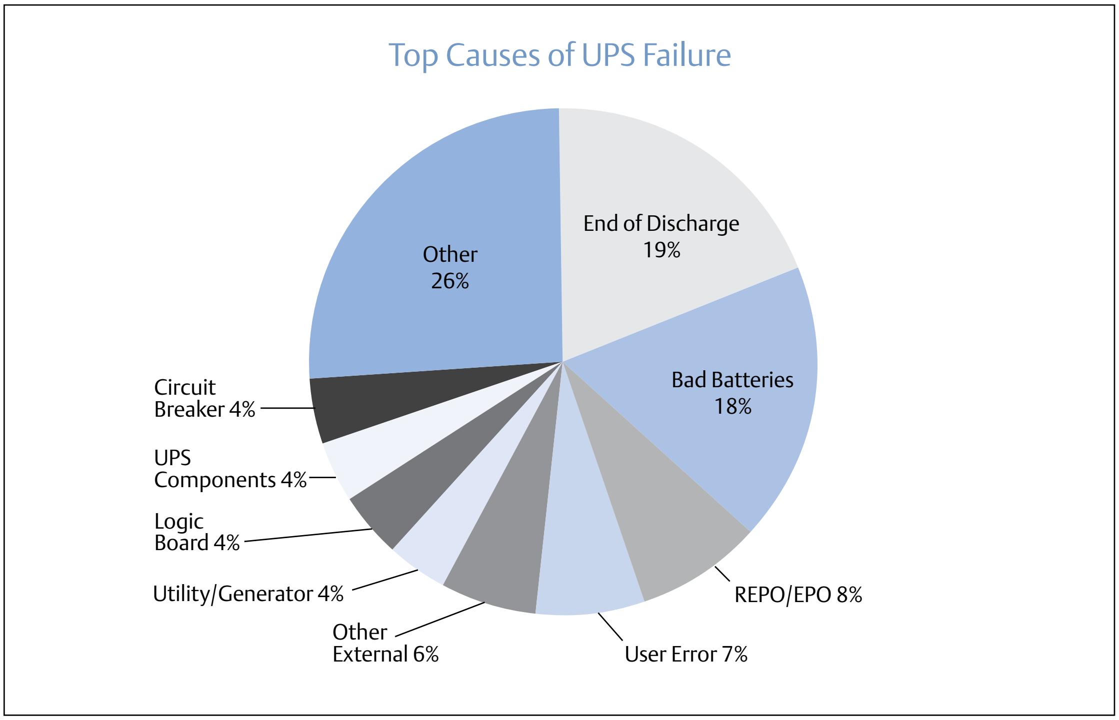

Figure 12. Battery problems (37 percent) represent the largest cause of UPS failure and can be minimized through UPS consolidation or remote battery monitoring.

Organizations with business-critical applications will likely benefit from dual bus redundancy, which creates parallel power paths to eliminate single points of failure. Organizations that are only concerned about utility power loss may be able to function with a single true online UPS.

Conclusion

Network access rooms present a challenge as far as power and cooling are concerned. In this dynamic environment, it is important to size and scale the power and cooling solutions for flexibility and future growth. Organizations with business-critical applications will likely benefit from dual bus redundancy, which creates parallel power paths to eliminate single points of failure. Organizations that are only concerned about utility power loss may be able to function with a single true online UPS.

Whatever the level of power redundancy, the network access room must be properly cooled and ventilated because heat will not dissipate and will be drawn back into the rack if it is not removed. To keep equipment operating at peak performance, a variety of remote monitoring and management software is available that can detect environment and equipment changes before adverse trends turn into emergencies. Organizations can also benefit from preventive maintenance and service agreements, including extended warranties that are cost effective and can help lengthen the life of the UPS.

Appendix A

Network Access Room Review Checklist

AVAILABILITY CONSIDERATIONS		
	YES	**NO**
Do you know what level of power availability you require in your network access room?	☐	☐
If not, have you calculated your cost of downtime for network access room equipment to help determine your desired availability level?	☐	☐
PHYSICAL ENVIRONMENT CONSIDERATIONS		
Physical Size	**YES**	**NO**
Can you fit all your desired network equipment - including power and cooling systems – into the rack?	☐	☐
Can you fit the rack into the room?	☐	☐
Existing Power	**YES**	**NO**
Is there sufficient incoming power for your full equipment loads?	☐	☐
Are there sufficient circuits for redundancy if desired?	☐	☐
Have you checked which types of receptacles are present – will they accommodate equipment plugs types?	☐	☐
Existing Cooling and Ventilation	**YES**	**NO**
Is the room ventilated?	☐	☐
If not, can it be ventilated to the outside?	☐	☐
Does room cooling – dedicated or building cooling – exist?	☐	☐
APPLICATION AND HARDWARE CONSIDERATIONS		
Power Quality	**YES**	**NO**
Will you equipment need power protection during outages only or continual protection and conditioning?	☐	☐
Power Reliability – Backup Runtime	**YES**	**NO**
Are you using full loads and not nominal loads to size the UPS?	☐	☐
Have you sized the UPS based on factors such as Power over Ethernet, network equipment growth, and the criticality of the equipment?	☐	☐
Power Reliability - Distribution	**YES**	**NO**
Do you require basic rack PDUs – those with multiple receptacles?	☐	☐
Do you require rack PDUs with monitoring and control capabilities?	☐	☐
Do you need to maintain tighter controls over who makes equipment changes?	☐	☐
What levels of power and UPS redundancy do you need given the criticality of your equipment and your cost of downtime?	☐	☐

Power Reliability – Power Redundancy	YES	NO
What levels of power and UPS redundancy do you need given the criticality of your equipment and your cost of downtime?	☐	☐
Physical Security	**YES**	**NO**
Is your network access room secure from physical entry?	☐	☐
Do you need to secure cabinets from unauthorized entry?	☐	☐
Do you want to be alerted when the cabinet is opened?	☐	☐
Cooling and Ventilation	**YES**	**NO**
Will the equipment you install require dedicated cooling equipment?	☐	☐
Is power consumption 4kW or more - high enough to consider high-density dedicated cooling?	☐	☐
What are the cooling requirements of your network equipment – planned and anticipated?	☐	☐
Monitoring & Management	**YES**	**NO**
Do you use network communications software?	☐	☐
Do you want to monitor power and cooling equipment via your network?	☐	☐
Do you want to be able to send alerts, initiate graceful shutdowns of equipment or and control power usage within the rack?	☐	☐
Preventative Maintenance & Rapid Response Service	**YES**	**NO**
Do you want to be able to service the UPS without shutting down power to the protected equipment?	☐	☐
Do you want to protect your UPSs with warranties beyond 2 years?	☐	☐
Do you need UPS and battery checks or other types of preventative maintenance?	☐	☐
Do you need startup services for larger UPSs and cooling systems?	☐	☐
Do you want to consider a long-term warranty and service package to provide preventative maintenance and repair for up to 5 years?	☐	☐

Emerson Network Power
1050 Dearborn Drive
P.O. Box 29186
Columbus, Ohio 43229
800.877.9222 (U.S. & Canada Only)
614.888.0246 (Outside U.S.)
Fax: 614.841.6022

EmersonNetworkPower.com
Liebert.com

WP160-58
SL-24624